República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(11) (21) **PI 9903609-6 A**

(22) Data de Depósito: 27/08/1999
(43) Data de Publicação: **24/04/2001**
(RPI 1581)

(51) Int. Cl[7].:
H04L 9/06

(54) Título: **PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA- HIPCRYPTO**

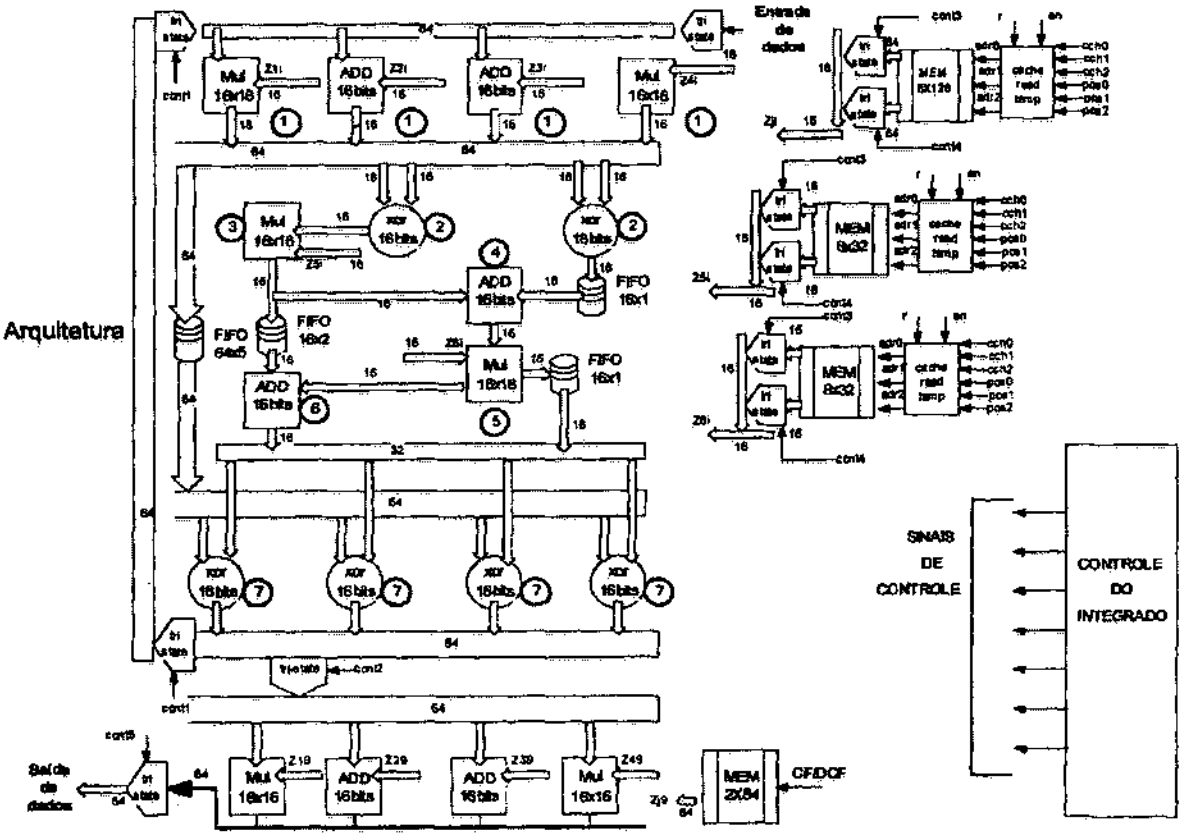
(71) Depositante(s): Coppe/Ufrj-Coordenação Dos Programas De Pós Graduação De Engenheira Da Universidade Federal Do Rio De Janeiro (BR/RJ)

(72) Inventor(es): Sérgio Luiz Cardoso Salomão, Sério Luiz Cardoso Salomão, Eliseu Monteiro Chaves Filho

(74) Procurador: Joubert Gonçalves De Casro & Zuldech Assessoria Empresarial Ltda

(57) Resumo: Patente de Invenção "PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO". O HIPCrypto é a implementação em hardware do algoritmo de chave privada considerado mais seguro na atualidade, o algoritmo IDEA (International Data Encriyption Algorithm), através da exploração das técnicas de paralelismo espacial e temporal, de forma a atender as velocidades de processamento requeridas pelas redes do tipo ATM.

Arquitetura



PI9903b09

Relatório Descritivo da Patente de Invenção "PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO".

CAMPO TÉCNICO

O HIPCrypto é uma proposta de arquitetura de hardware para o algoritmo criptográfico IDEA, patenteado nos EUA sob o no. US05214703 na qual foram utilizadas as técnicas de exploração de paralelismo espacial e temporal, de maneira a permitir que o HIPCrypto atinja as velocidades de processamentos requeridas pelas redes do tipo ATM.

Atualmente existe uma tendência mundial para a utilização de redes de telecomunicações mais universais, ou seja, redes que atendam a diferentes tipos de serviços em Telecomunicações (Redes de Serviços Integrados). Estes tipos de redes devem atender desde a serviços que requeiram baixa capacidade de transmissão de dados (Telefonia Convencional, Telex, TV's a Cabo e Convencional, etc) até serviços que requeiram uma alta taxa de transmissão de dados (Vídeo conferência, Biblioteca de vídeos, etc).

Um primeiro passo para a Rede de Serviços Integrados surgiu com a criação da Rede Digital de Serviços Integrados de Banda estreita (RDSI-BE), capaz de integrar voz, dados e vídeo de baixa definição (com taxas de transmissão de 64 KBits/s até 2 MBits/s) em um acesso de Rede digital de voz. Entretanto, a RDSI-BE possui limitações, não podendo oferecer serviços que necessitem de altas velocidades de transmissão.

Uma Rede para ser considerada Universal deve suportar um largo número de serviços, tais como:

- Baixa velocidade (Telemetria, Telecontrole, Tele Alarme, Voz, Telefax, Transmissão de Dados de Baixa velocidade);

- Média Velocidade (hi-fi sound, vídeo telefonia, etc);

- Alta velocidade (Distribuição de vídeo de alta qualidade, Biblioteca de vídeos, etc).

Desta forma, o modo de transferência para esta Rede Universal não pode ser concebido especificamente para um tipo de serviço, pois estima-se taxas de transmissão de poucos bits/s até algumas centenas de MBits/s. Claramente faz-se necessário uma rede de alta performance e alta velocidade. Este é o objetivo da Rede Digital de Serviços Integrados de Banda Larga (RDSI-BL) .

O ITU-T (International Telecommunication Union) é o órgão responsável pelas recomendações (Padrões) da Rede Digital de Serviço Integrados e adotou o Modo de Transferência Assíncrono (ATM-Asynchronous Transfer Mode) como solução para a implementação de Rede RDSI-BL devido às vantagens nas características dos serviços que esta tecnologia objetiva oferecer tais como flexibilidade, independência da taxa de transmissão e comutação de todos os serviços em uma única estrutura.

A tecnologia ATM é capaz de suportar diferentes serviços para satisfazer aos requisitos exigidos pelos diferentes tipos de tráfego e altas velocidades de transmissão.

Existem também atualmente redes que atingem taxas de transmissão da ordem de Giga Bits/s, conhecidas genericamente como Redes de GIGA Bits/s. Estas redes

possuem a tendência de serem utilizadas em larga escala no futuro próximo.

Em paralelo ao avanço tecnológico das redes de transmissão de dados que além do avanço técnico se tornaram mais disseminadas, passou a existir a necessidade cada vez mais crescente da Segurança da integridade dos dados ou informações a serem transmitidas por estas Redes.

Isto ocasionou durante os últimos anos um avanço considerável da estrutura dos algoritmos criptográficos que passaram a ser utilizados pelas organizações que necessitam de segurança (Bancos, Governo, Indústria, etc). Estes algoritmos tornaram-se progressivamente mais robustos em relação a sua criptoanálise, ou seja, tornaram-se cada vez mais seguros, com chaves de cifragem e decifragem cada vez maiores e com operações internas de processamento cada vez mais complexas.

Estes algoritmos criptográficos devido as suas novas características, passaram a ter o seu processamento mais demorado, tanto devido ao número maior de operações internas necessárias a sua execução, como também ao tamanho dos dados e da chave código a serem processados, ocasionando uma preocupação mundial em relação a compatibilidade de velocidade de execução destes algoritmos e das redes de computadores a serem protegidas por estes.

Com o aparecimento das redes do tipo RDSI/BE ((64 KBits/s até 2 MBits/s e posteriormente das Redes do tipo ATM, que trabalha com taxas de transferência de dados de 150 MBits/s para operações típicas e até 620 MBits/s para operações mais específicas, este problema se agravou.

A solução adotada pela comunidade mundial foi a de tentar implementar estes algoritmos criptográficos em forma de circuitos integrados dedicados (ASICS) ou pelo menos as partes críticas em velocidade de processamento destes algoritmos em Hardware.

Estas tentativas surtiram efeito até alguns anos atrás, porém com o desenvolvimento de algoritmos criptográficos mais robustos e com a aparecimento das redes do tipo ATM (Principalmente das Redes de Giga Bits), este problema retornou com uma complexidade ainda maior.

TÉCNICAS ANTERIORES

Para fazer face ao aumento da velocidade de processamento dos sistemas computacionais e principalmente do aumento da velocidade das redes de transmissão de dados, tendo em vista a extrema necessidade atual de segurança na transmissão de informações, é que muitos algoritmos criptográficos passaram a ser implementados em forma de circuitos dedicados (ASICs), ou tiveram as suas partes mais críticas em termos de velocidade implementadas com esta metodologia.

O algoritmo criptográfico mais difundido de chave única, o DES (Data Encrytion Standard), possui varias versões desenvolvidas em hardware. Devido a sua vasta exploração vários desempenhos computacionais para este algoritmo são conhecidos. O DES cifra blocos de 64 bits usando uma chave de 56 bits com mais 8 bits de paridade, ou seja, utiliza uma pseudo chave de 64 bits.

Inicialmente o DES foi implementado sobre uma máquina que utilizava um microprocessador 8088, com freqüência de operação de 4.7 MHz. Esta implementação obteve um desempenho computacional de 370 blocos de 64 bits

por segundo, ou melhor 23,68 Kbits/s. Este mesmo algoritmo implementado sobre um microprocessador 80486, com em 66 MHz, atinge uma velocidade de processamento de 2,752 Mbits/s. Umas das maiores velocidades de processamento para este algoritmo, até a algum tempo atrás, era quando este era processado sobre um computador HP9000/887, cuja velocidade de processamento atinge 10,816 Mbits/s. A tabela 1 mostra alguns desempenhos para o algoritmo DES sobre diferentes plataformas computacionais.

Foram desenvolvidas e implementadas comercialmente para o algoritmo DES, durante as últimas duas décadas, várias versões em hardware deste algoritmo. O primeiro integrado a surgir foi o Am9518, desenvolvido pela AMD em 1981 que utilizava uma freqüência de operação de 3 MHz, com uma velocidade de processamento (taxa de cifragem) de 1,3 Mbytes/s (10,4 Mbits/s). A última versão em hardware do algoritmo DES que se tem conhecimento é o chip 6868, desenvolvido em 1995 pela VLSI technology, cuja velocidade de processamento de dados para cifragem ou decifragem é de 512 Mbits/s. Na tabela 2 encontramos as principais implementações do algoritmo criptográfico DES em hardware com seus respectivos fabricantes e desempenhos.

Observando as tabelas 1 e 2, verificamos que a primeira implementação em hardware do DES, o AM9538, tem praticamente a mesma velocidade de processamento de dados do melhor desempenho de software mostrado na tabela 1, o que nos mostra a clara superioridade em termos de velocidade, das implementações em hardware.

Observando ainda a tabela 2, verificamos que o melhor desempenho em hardware foi obtido com o integrado 6868 da VLSI Thecnology. A velocidade obtida de

processamento de dados de 512 Mbits/s atende à maioria das aplicações das redes do tipo ATM. Contudo, além de não atender à todas aplicações das redes do tipo ATM e às redes de Giga-bits, este algoritmo já é considerado ultrapassado, se levarmos em consideração os novos algoritmos de chave privada como é o algoritmo IDEA.

Para a família de algoritmos criptográficos que originaram o IDEA, poucas implementações são do nosso conhecimento. Uma das implementações em hardware conhecida foi desenvolvida para executar o algoritmo PES, o percursor do IDEA. Este integrado obteve uma velocidade de processamento de dados, para a cifragem ou a decifragem, de 55 Mbits/s, a uma freqüência de operação de 25 MHz .

DESCRIÇÃO DETALHADA

Algoritmo Criptográfico IDEA

A primeira forma do algoritmo IDEA, criada por "Xuejia Lai e James Massey", foi em 1990 (patente US05214703) e foi chamada de PES (Proposed Encryption Standard). No ano seguinte, após Bihan e Shamir's demonstrarem a criptoanalise diferencial, o algoritmo foi fortalecido e passou a se chamar IPES (Improved Proposed Encryption Standard).O IPES mudou de nome em 1992 e passou a se chamar IDEA (International Data Encryption Algorithm), que é considerado por muitos como o melhor e mais seguro algoritmo simétrico da atualidade.

O algoritmo IDEA, figura 1, opera com dados de entrada de 64 bits e possui a chave de cifragem (decifragem) de 128 bits. Estes dados, juntos com a chave, sofrem operações algébricas do tipo:

XOR, adição ao módulo 2^{16} (adição, ignorando o "overflow"), multiplicação ao módulo $2^{16} + 1$ (

multiplicação, ignorando o "overflow"), todas estas operações são em 16 bits.

O algoritmo recebe os 64 bits de dados e os divide em 4 blocos de 16 bits cada um , blocos X1 , X2 , X3 e X4. Estes 4 blocos serão a entrada da primeira fase do algoritmo. Existem 8 fases no total.

Em cada fase cada um dos 4 blocos de entrada sofre operações de soma , multiplicação e ou exclusivo , cada um com o outro e com os 6 blocos de 16 bits do código chave: $Z1^{(i)}$, $Z2^{(i)}$, $Z3^{(i)}$, $Z4^{(i)}$, $Z5^{(i)}$ e $Z6^{(i)}$. Entre cada fase , o segundo e o terceiro blocos da saída são trocados. Em cada fase a seqüência de eventos é a seguinte:

1 - Multiplicação entre X1 e o primeiro bloco do código chave $Z1^{(1)}$.

2 - Adição entre X2 e o segundo bloco do código chave $Z2^{(1)}$.

3 - Adição entre X3 e o terceiro bloco do código chave $Z3^{(1)}$.

4 - Multiplicação entre X4 e o quarto bloco do código chave $Z4^{(1)}$.

5 - Operação de ou exclusivo entre os resultados de (1) e (3).

6 - Operação de ou exclusivo entre os resultados de (2) e (4).

7 - Multiplicação entre o resultado de (5) e o quinto bloco do código chave $Z5^{(1)}$.

8 - Adição dos resultados de (6) e (7).

9 - Multiplicação entre o resultado de (8) e o sexto bloco do código chave $Z6^{(1)}$.

10 - Adição dos resultados de (7) e (9).

11 - Operação de ou exclusivo entre os resultados de (1) e (9).

12 - Operação de ou exclusivo entre os resultados de (3) e (9).

13 - Operação de ou exclusivo entre os resultados de (2) e (10).

14 - Operação de ou exclusivo entre os resultados de (4) e (10).

A saída desta fase são os quatros blocos resultantes em (11) , (12) , (13) e (14). Troca-se de posição os dois blocos interiores (exceto para a fase final), ou seja , o segundo e o terceiro blocos obtidos. Estes blocos agora funcionam como a entrada para a próxima fase, correspondendo do primeiro ao quarto na seguinte ordem: (11) , (13) , (12) e (14). Este procedimento se repete por todas as oito fases, apenas rendo em cada fase blocos de código chave de 16 bits diferentes.

Após a execução das oito fases, os blocos de dados, X1, X2, X3 e X4, finalmente sofrem a transformada de saída no estágio de saída:

15 - Multiplicação entre X1 e o primeiro bloco de código chave da nona fase, $Z1^{(9)}$.

16 - Adição entre X2 e o segundo bloco de código chave da nona fase, $Z2^{(9)}$.

17 - Adição entre X3 e o terceiro bloco de código chave da nona fase, $Z3^{(9)}$.

18- Multiplicação entre X4 e o quarto bloco de código chave da nona fase, $Z4^{(9)}$.

O algoritmo utiliza 52 blocos de código chave de 16 bits, 6 para cada um das 8 fases e 4 para a nona

fase. Estas chaves são obtidas a partir da chave longa de 128 bits.

Inicialmente, os 128 bits da chave são divididos em oito blocos de 16 bits:

Os seis primeiros blocos de 16 bits (K1 a K6) eqüivalem respectivamente às seis chaves de 16 bits para a primeira fase($Z1^{(1)}$ a $Z6^{(1)}$). Os dois blocos que sobram, K7 e K8, correspondem a primeira e a segunda chave de 16 bits para a segunda fase, $Z1^{(2)}$ e $Z2^{(2)}$.

A seguir, a chave de 128 bits sofre uma rotação de 25 bits a esquerda. A nova chave de 128 bits obtida após esta operação e novamente dividida em oito blocos de 16 bits.

Os quatro primeiros blocos são as quatro chaves de 16 bits que faltavam para a segunda fase, $Z3^{(2)}$, $Z4^{(2)}$, $Z5^{(2)}$ e $Z6^{(2)}$. Os quatro blocos restantes são as quatro primeiras chaves da terceira fase, $Z1^{(3)}$, $Z2^{(3)}$, $Z3^{(3)}$ e $Z4^{(3)}$.

A chave de 128 bits é novamente rotacionada de 25 posições a esquerda e dividida em novos oito blocos de 16 bits. Este procedimento se repete até que as 52 chaves de 16 bits para o algoritmo de cifragem tenham sido geradas.

O processo de decifragem do algoritmo IDEA é essencialmente o mesmo que o processo de cifragem. As chaves de decifragem são as chaves de cifragem aplicadas em ordem reversa, vide tabela 1. $Z^{(i)\,-\,1}$ denota a inversa multiplicativa de $Z^{(i)}$ ao módulo $2^{16} + 1$, isto é, $Z^{(i)\,-\,1} \times Z^{(i)} = 1$. $-Z^{(i)}$ denota a inversa aditiva de $Z^{(i)}$, isto é, $-Z^{(i)} + Z^{(i)} = 0$.

Exploração do paralelismo espacial e temporal

Após um estudo aprofundado do algoritmo, foi obtido o seguinte paralelismo espacial (figura 2):

- As operações contidas em 1, 2, 3 e 4, da descrição das operações do algoritmo IDEA, podem ser executadas paralelamente, ou seja, em um único ciclo de máquina, bastando para tanto o uso de duas estruturas multiplicadoras de 16 bits e duas estruturas somadoras de 16 bits. Os dados que concorrem a estas operações, os 64 bits de dados e as subchaves código Z1, Z2, Z3 e Z4, são independentes e podem ser fornecidos ao mesmo tempo.

- As operações 5 e 6 também podem ser executadas em um único ciclo de máquina, bastando para isso duas estruturas ou-exclusivo de 16 bits, pois os dados que concorrem a estas operações são os resultados das operações 1, 2, 3 e 4.

- As operações 7, 8, 9 e 10 devem ser executadas em ciclos de máquina diferentes, pois estas dependem de dados seqüenciais não concorrentes no tempo para a sua execução, pois:

• A operação 7 depende do resultado da operação 5 e da subchave código Z5.

• A operação 8 depende do resultado da operação 6 e da operação 7, não podendo desta forma ocorrer no mesmo ciclo de máquina da operação 7.

• A operação 9 depende do resultado da operação 8 e da subchave código Z6, não podendo ser realizada no mesmo ciclo de máquina da operação 8.

• A operação 10 depende do resultado da operação 7 e da operação 9 e da mesma forma não pode ser realizada no mesmo ciclo de máquina da operação 9.

Finalmente, as operações 11, 12, 13 e 14 podem ser executadas no mesmo ciclo de máquina, com a utilização de duas estruturas ou-exclusivo de 16 bits em paralelo, bastando para isso o armazenamento dos resultados das operações 1, 2, 3 e 4 e o resultado das operações 9 e 10.

O estágio de saída também pode ser executado em um único ciclo de máquina, com uma estrutura paralela de dois multiplicadores de 16 bits e dois somadores de 16 bits.

Este é o paralelismo espacial máximo obtido para o algoritmo IDEA. A seguir cada estágio do paralelismo obtido foi transformado em um segmentos de uma estrutura pipeline (paralelismo temporal), conforme figura 2, ou seja;

- O estágio 1 do paralelismo, com as operações 1, 2, 3 e 4, será o primeiro segmento da estrutura pipeline.

- O estágio 2 do paralelismo, com as operações 5 e 6, será o segundo segmento da estrutura pipeline.

- O estágio 3 do paralelismo, com a operação 7, será o terceiro segmento da estrutura pipeline.

- O estágio 4 do paralelismo, com a operação 8, será o quarto segmento da estrutura pipeline.

- O estágio 5 do paralelismo, com a operação 9, será o quinto segmento da estrutura pipeline.

- O estágio 6 do paralelismo, com a operação 10, será o sexto segmento da estrutura pipeline.

- O estágio 7 do paralelismo, com as operações 11, 12, 13 e 14, será o sétimo segmento da estrutura pipeline.

Arquitetura do HIPCrypto

• A arquitetura do HIPCrypto, conforme figura 3, executa uma fase completa do algoritmo mais o estágio de saída, dando um total de 6 multiplicadores de 16 bits, 6 somadores de 16 bits e 6 estruturas ou-exclusivo de 16 bits, memórias, buffers, tri-states e uma unidade de controle.

• As operações contidas em cada segmento da estrutura pipeline, serão executadas em um único ciclo de máquina e como são 7 os segmentos do pipeline, o integrado irá cifrar (decifrar) 7 blocos de 64 bits por execução do algoritmo.

• O integrado foi projetado de forma a permitir que este possa ser cascateado com outro(s) integrado(s) HIPCryptos, ou seja, que sejam permitidas as configurações em série de 1, 2, 4 ou 8 integrados.

• As 4 configurações possíveis, em relação ao número de fases do algoritmo criptográfico IDEA, que cada integrado HIPCrypto passará a executar ao ser cascateado a outro integrado, funcionarão de acordo com a tabela 3.

• Como cada segmento do pipeline será executado a cada ciclo de máquina, para as diferentes configurações possíveis teremos o seguinte processamento: para a configuração de 1 integrado teremos o processamento de 7 blocos de 64 bits a cada 56 (7 x 8) ciclos de máquina, para 2 integrados teremos o processamento de 7 blocos de 64 bits a cada 28 (7 x 4) ciclos de máquina, para 4 integrados

teremos o processamento de 7 blocos de 64 bits a cada 14 (7 x 2) ciclos de máquina, para 8 integrados teremos o processamento de 7 blocos de 64 bits a cada 7 (7 x 1) ciclos de máquina, ou seja, 1 bloco de 64 bits a cada ciclo de máquina. Desta forma quanto maior o número de integrados utilizados maior será a profundidade do pipeline em relação as fases de execução do algoritmo, ou seja, maior será a latência do circuito.

A estrutura proposta para o integrado HIPCrypto foi adequada às várias utilizações possíveis, deixando a cargo de cada utilização o compromisso entre velocidade e custo, isto é, quanto maior a velocidade desejada para a aplicação, maior será o custo do hardware.

Os sinais responsáveis pela escolha da configuração do integrado foram divididos em dois grupos: três sinais que definirão a configuração do integrado cch <2:0> (configuração do chip) e três sinais que definirão a posição do integrado em relação a cadeia de integrados em série definidas por cada configuração adotada, pos <2:0> (posição do chip). A tabelas 4 e 5 nos fornecem respectivamente as configurações e as posições possíveis para o HIPCrypto referentes aos níveis lógicos dos sinais de seleção.

É importante notar que as oito posições só são possíveis para a configuração de oito integrados, ou seja:

• Para um integrado só é possível a primeira configuração.

• para dois integrados só são possíveis as duas primeiras configurações.

• E para quatro integrado só são possíveis as quatro primeiras configurações.

Para um melhor entendimento desta associação, na tabela 6 mostramos como estes sinais estão relacionados.

Esta estrutura proposta para a seleção das configurações do integrado tem o intuito de permitir a modularidade do mesmo, ou seja, que um integrado possa ser facilmente substituído por outro qualquer que seja a configuração utilizada e qualquer que seja a posição deste na configuração, sendo somente necessário que os sinais de seleção de configuração sejam ativados corretamente.

As subchaves de 16 bits são armazenadas em 4 memória RAM´s conforme figura 4 e mais detalhadamente na figura 3..

Para as subchaves $Z1^{(i)}$, $Z2^{(T)}$, $Z3^{(i)}$ e $Z4^{(i)}$, uma memória de 128 bits por 8 posições. Os primeiros 64 bits de cada posição de dados da memória, bits menos significativos, armazenam as subchaves código de cifragem (posições 0 a 63) e os últimos 64 bits, bits mais significativos (posições 64 a 127), armazenam as subchaves de decifragem. A seleção para executar o algoritmo em modo cifragem ou decifragem é feita através da liberação para o barramento das subchaves, que irão interagir com o primeiro segmento do pipeline, da parte inferior ou superior do barramento de dados da memória.

Para as subchaves $Z5^{(i)}$ e $Z6^{(i)}$, duas memórias de 32 bits por 8 posições, onde os 16 bits menos significativos de cada posição de memória (bits de 0 a 15), armazenam as subchaves chaves de cifragem $Z5^{(i)}$ e $Z6^{(i)}$, uma em cada memória, e os 16 bits mais significativos armazenam as subchaves de decifragem. A seleção do modo de operação

do integrado, cifragem ou decifragem, tem procedimento idêntico ao descrito anteriormente

Para as subchaves $Z1^{(9)}$, $Z2^{(9)}$, $Z3^{(9)}$ e $Z4^{(9)}$, uma memória de 64 bits por 2 posições, sendo que na primeira posição de memória ficam armazenadas as subchaves de cifragem e na segunda posição as subchaves de decifragem.

Unidade de controle

A unidade de controle, figura 3, é o bloco operacional que controla o funcionamento da arquitetura. Esta unidade em conjunto com alguns circuitos extras é responsável pelo gerenciamento dos sinais que controlam o HIPCrypto. As principais funções desta unidade são descritas a seguir.

A partir da seleção do modo de operação do integrado (cifragem/decifragem), a unidade de controle habilita os sinais de controle responsáveis por essa seleção. Para o HIPCrypto, o algoritmo de cifragem é idêntico ao algoritmo de decifragem, diferenciando apenas as subchaves código utilizadas em cada caso. Logo, o que a unidade de controle faz é habilitar as chaves códigos de cifragem ou as chaves códigos de decifragem armazenadas nas memórias contidas na arquitetura.

Para as três primeiras memórias, que atendem aos segmentos 1, 3 e 5 da estrutura pipeline, figura 2, a unidade de controle habilita para a leitura ou os bits de dados menos significativos (cifragem) ou os bits de dados mais significativos (decifragem). Para a memória que atende o estágio de saída, a unidade de controle habilita ou a primeira posição de memória (cifragem) ou a segunda posição

de memória (decifragem). A seleção é feita através de circuitos tristates.

A unidade de controle também permiti a inicialização das operações no integrado, isto é, permitir de forma correta o preenchimento da estrutura pipeline. A cada início de uma operação de cifragem ou decifragem, em qualquer configuração escolhida, os dados de 64 bits a serem processados entram seqüencialmente no integrado até o preenchimento dos 7 segmentos da estrutura pipeline. Sendo assim, é necessário que os circuitos existentes em cada um dos 7 segmentos, inclusive as memórias, funcionem apenas quando existirem dados a serem processados por estes, permitindo desta forma que os segmentos operem sincronizados.

Como no HIPCrypto cada um dos segmentos do pipeline realiza suas operações em um ciclo de máquina, temos que os atrasos de início de funcionamento de cada um dos segmentos, pode ser dado como um ciclo de máquina, ou seja, os circuitos do segundo segmento do pipeline só serão ativados um ciclo de máquina após os circuitos do primeiro segmento terem sido ativados, os circuitos do terceiro segmento serão ativados um ciclo de máquina após os do segundo segmento terem sido ativados ou dois ciclos após os do primeiro segmento terem sido ativados e assim sucessivamente.

A unidade de controle age em diversas partes do circuito, em sinais como "resets" e "enable's", de maneira a permitir a implementação desta inicialização.

Uma das funções principais da unidade de controle é o gerenciamento do fluxo de dados do integrado,

ou seja, o controle da entrada e saída de dados a serem processados. Esta parte do controle deverá identificar:

• A existência de dados a serem processados pelo integrado.

• O número de fases do algoritmo que o integrado integrado deverá executar.

• Se o estágio de saída será utilizado ou não.

• Se existe algum integrado em série com o seu integrado, avisando-o de um provável envio de dados.

• O fim de uma operação de cifragem ou decifragem.

A existência de dados a serem processados será reconhecida pela unidade de controle através de um sinal externo ao integrado chamado "temdados", vindo do barramento de dados.

O número de fases do algoritmo que o integrado deverá executar, refere-se a configuração a qual o integrado está submetido (1, 2, 4 ou 8 fases). Caso o integrado necessite realizar mais de uma fase do algoritmo, é necessário que os dados que se apresentem na saída do sétimo segmento do pipeline sejam realimentados para a entrada do primeiro segmento do pipeline, de maneira que este possa realizar mais uma fase do algoritmo sobre os dados que estão sendo processados.

O estágio de saída só será utilizado pelo último integrado de cada configuração. Desta forma se faz necessário que a unidade de controle de cada integrado identifique se o seu integrado utilizará ou não o estágio de saída, ou seja se o seu integrado é o ultimo da configuração adotada ou não.

Desempenho do HIPCrypto

Um exemplo para o desempenho do HIPCrypto é a sua implementação em tecnologia CMOS 0,7 micron com dois níveis de metalização, cujo desempenho para as diversas configurações é mostrado na tabela 7.

PI9903805

REIVINDICAÇÕES

1 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, que compreende um método para a utilização do algoritmo de chave simétrica intitulado IDEA, caracterizado por fazer uso de um pipeline de sete estágios a ser implementado sob forma de um circuito síncrono, que será denominado micro-pipeline, acoplado a um estágio de saída conforme descrito na figura 2; sendo que cada estágio do pipeline fornece resultados parciais para o estágio seguinte e colhe resultados parciais do estágio anterior a cada pulso de relógio do circuito síncrono; existindo uma realimentação do estágio de número 7 para o estágio de número 1, controlada pela unidade de controle digital de forma que, a cada uma das 16 rodadas necessárias para a cifragem de um bloco de 64 bits, o primeiro estágio do pipeline seja alimentado com resultados parciais provindos da saída do sétimo estágio de pipeline e que o pipeline seja alimentado com um novo bloco para cifragem quando o processo de cifragem estiver concluído; sendo que as sub-chaves usadas nos processos de cifragem e decifragem de dados, de acordo com a definição do algoritmo IDEA, são armazenadas em quatro unidades de memória dedicadas a este fim.

2 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual as operações 1, 2, 3 e 4 da descrição do algoritmo criptográfico IDEA são executadas por duas unidades multiplicadoras de 16 bits e duas unidades somadoras de 16 bits; sendo que estas unidades compoem o estágio de número um do pipeline conforme descrito na figura 2; recebendo

este estágio, seja um novo bloco de 64 bits proveniente da entrada de dados seja um resultado parcial do sétimo estágio e as sub-chaves de cifragem ou decifragem correspondentes a este estágio conforme descrito nas figuras 2 e 3; sendo as entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

3 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual as operações 5 e 6 da descrição do algoritmo criptográfico IDEA são executadas por duas unidades de ou-exclusivos de 16 bits; sendo que estas unidades compoem o estágio de número dois do pipeline conforme descrito na figura 2; recebendo este estágio, resultados parciais do primeiro conforme descrito nas figuras 2 e 3; sendo as entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

4 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual a operação 7 da descrição do algoritmo criptográfico IDEA é executada por uma unidade multiplicadora de 16 bits; sendo que esta unidade compoem o estágio de número três do pipeline conforme descrito na figura 2; recebendo este estágio, resultados parciais do estágio anterior e as sub-chaves de cifragem ou decifragem correspondentes a este estágio conforme descrito nas figuras 2 e 3; sendo as

entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

5 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual a operação 8 da descrição do algoritmo criptográfico IDEA é executada por uma unidade somadora de 16 bits; sendo que esta unidade compõe o estágio de número quatro do pipeline conforme descrito na figura 2; recebendo este estágio, resultados parciais dos estágios 2 e 3 conforme descrito na figura 2; sendo as entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

6 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual a operação 9 da descrição do algoritmo criptográfico IDEA é executada por uma unidade multiplicadora de 16 bits; sendo que esta unidade compoem o estágio de número cinco do pipeline conforme descrito na figura 2; recebendo este estágio, resultados parciais do estágio anterior e as sub-chaves de cifragem ou decifragem correspondentes a este estágio conforme descrito nas figuras 2 e 3; sendo as entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

7 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual a operação 10 da descrição do algoritmo criptográfico IDEA é

executada por uma unidade somadora de 16 bits; sendo que esta unidade compõe o estágio de número seis do pipeline conforme descrito na figura 2; recebendo este estágio resultados parciais dos estágios 3 e 5 conforme descrito na figura 2; sendo as entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

8 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método no qual as operações 11, 12, 13 e 14 da descrição do algoritmo criptográfico IDEA são executadas por quatro unidades de ou-exclusivos de 16 bits; sendo que estas unidades compoem o estágio de número sete do pipeline conforme descrito na figura 2; recebendo este estágio, resultados parciais dos estágios 1, 5 e 6 conforme descrito na figura 2; sendo as entradas e saídas deste estágio ligadas a registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

9 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser o método no qual as operações 15, 16, 17 e 18 da descrição do algoritmo criptográfico IDEA são executadas por duas unidades multiplicadoras de 16 bits e por duas unidades somadoras de 16 bits; sendo que estas unidades compoem o estágio de saída do pipeline conforme descrito na figura 2; recebendo este estágio, resultados parciais do estágio 7 do pipeline e as sub-chaves de cifragem ou decifragem correspondentes ao estágio de saída conforme descrito nas figuras 2 e 3; sendo as entradas e saídas deste estágio ligadas a

registradores usados para memorização de dados que o estágio fornece e recebe ao fim de cada período de relógio.

10 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com a reivindicação 1, caracterizado por ser um método em que as sub-chaves usadas no processo de cifragem e de decifragem são armazenadas em quatro memórias dedicadas conforme a figura 4 e da seguinte forma: sub-chaves $Z1^{(i)}$, $Z2^{(i)}$, $Z3^{(i)}$ e $Z4^{(i)}$ de cifragem (i de 1 a 8) e as sub-chaves $Z1^{(i)}$, $Z2^{(i)}$, $Z3^{(i)}$ e $Z4^{(i)}$ de decifragem (i de 1 a 8) armazenadas na memória de 128 bits x 8 posições; as sub-chaves de cifragem $Z5^{(i)}$ (i de 1 a 8) e as sub-chaves de decifragem $Z5^{(i)}$ (i de 1 a 8) armazenadas na primeira memória de 32 bits x 8 posições; as sub-chaves de cifragem $Z6^{(i)}$ (i de 1 a 8) e as sub-chaves de decifragem $Z6^{(i)}$ (i de 1 a 8) armazenadas na segunda memória de 32 bits x 8 posições; as sub-chaves de cifragem $Z1^{(9)}$, $Z2^{(9)}$, $Z3^{(9)}$ e $Z4^{(9)}$ e as subchaves de decifragem $Z1^{(9)}$, $Z2^{(9)}$, $Z3^{(9)}$ e $Z4^{(9)}$ armazenadas na memória de 64 bits x 2 posições.

11 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com as reivindicações 1 e 2, caracterizado por ser o método pelo qual usa-se um segundo nível de pipeline, denominado macro-pipeline, que permite concatenar 2, 4 ou 8 circuitos operando com um micro-pipeline de sete estágios conforme indicado na tabela 3.

12 - PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO, de acordo com as reivindicações 1 e 2, caracterizado por ser o método pelo qual usam-se memórias do tipo "first-in first-out", (FIFO) para sincronizar os dados oriundos de estágios não

adjacentes da seguinte forma: uma FIFO de 64 bits x 5 posições interligando os estágios 1 e 7, uma FIFO de 16 bits x 2 posições interligando os estágios 3 e 6, uma FIFO de 16 bits x 1 posição interligando os estágios 2 e 4, uma FIFO de 16 bits x 1 posição interligando os estágios 5 e 7, conforme descrito na figura 3.

FIGURAS

Tabela 1

Velocidade do algoritmo DES implementado em diferentes plataformas.

Plataforma	Freqüência de operação (MHz)	Taxa de cifragem
8088	4,7	23,68 Kbits/s
68000	7,6	57,6Kbits/s
80286	6	70,4 Kbits/s
68020	16	224 Kbits/s
68030	16	249,6 Kbits/
80386	25	320 Kbits/s
68030	50	640 Kbits/s
68040	25	1,024 Mbits/s
68040	40	1,472 Mbits/s
80486	66	2,752 Mbits/s
HP900/887	125	10,816 Mbits/s
Sun ELC		1,664 Mbits/s
HyperSparc		2,048 Mbits/s
RS6000-350		3,392 Mbits/s
Sparc 10/52		5,376 Mbits/s
DEC Alpha 4000/610		9,856 Mbits/s

Tabela 2

Integrados comerciais do algoritmo DES

Fabricante	Integrado	Ano de fabricação	Freqüência de operação	Velocidade (bits/s)
AMD	Am9518	1981	3 MHz	10,4 Mbits/s
AMD	Am9568	?	4 MHz	12 Mbits/s
AMD	AmZ8068	1982	4 MHz	13,6 Mbits/s
AT&T	T7000A	1985	?	15.2 Mbits/s
CE-infosys	SuperCrypt CE99C003	1992	20 MHz	100 Mbits/s
CE-infosys	SuperCrypt CE99C003A	1994	30 MHz	160 Mbits/s
Cryptech	Cry12C102	1989	20 MHz	22,4 Mbits/s
Newbridge	CA20C03A	1991	25 MHz	30,8 Mbits/s
Newbridge	CA20C03W	1992	8 MHz	5,12 Mbits/s
Newbridge	CA95C68/18/09	1993	33 MHz	117,4 Mbits/s
Pijnenburg	PCC100	?	?	20 Mbits/s
Semaphore Communications	Roadrunner284	?	40 Mhz	284 Mbits/s
VLSI technology	VM007	1993	32 MHz	160 Mbits/s
VLSI technology	VM009	1993	33 MHz	112 Mbits/s
VLSI technology	6868	1995	32 MHz	512 Mbits/s

Tabela 3

Configuração	numero de fases do algoritmo executadas em cada integrado
1 integrado	8 fases executadas
2 integrados	4 fases em cada integrado
4 integrados	2 fases em cada integrado
8 integrados	1 fase em cada integrado

Tabela 4:

ch2	ch1	ch0	Configuração
			1 integrado.
			2 integrados em série.
			4 integrados em série.
			8 integrados em série.

Tabela 5:

pos 2	pos 1	pos0	Posição do integrado.
0	0	0	Primeira posição
0	0	1	Segunda posição
0	1	0	Terceira posição
0	1	1	Quarta posição
1	0	0	Quinta posição
1	0	1	Sexta posição
1	1	0	Sétima posição
1	1	1	Oitava posição

Tabela 6:

Configuração			Posição		
cch2	cch1	cch0	pos2	pos1	pos0
0	0	0	0	0	0
0	0	1	0	0	0
			0	0	1
0	1	0	0	0	0
			0	0	1
			0	1	0
			0	1	1
1	0	0	0	0	0
			0	0	1
			0	1	0
			0	1	1
			1	0	0
			1	0	1
			1	1	0
			1	1	1

Tabela 7:

Configurações do macro-pipeline	Desempenhos Freq de relógio: (59 MHz)
1 integrado	472 Mbits/s
2 integrados	944 Mbits/s
4 integrados	1,888 Gbits/s

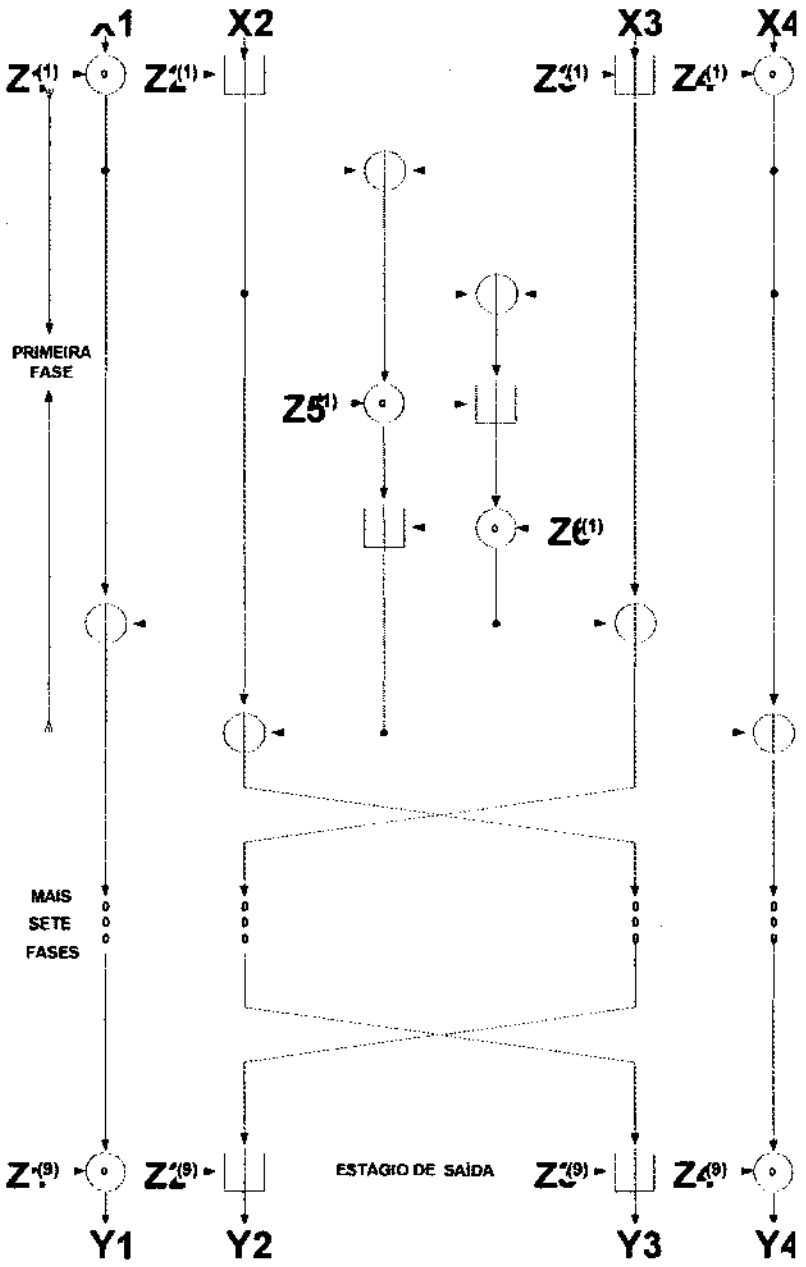


Figura 1

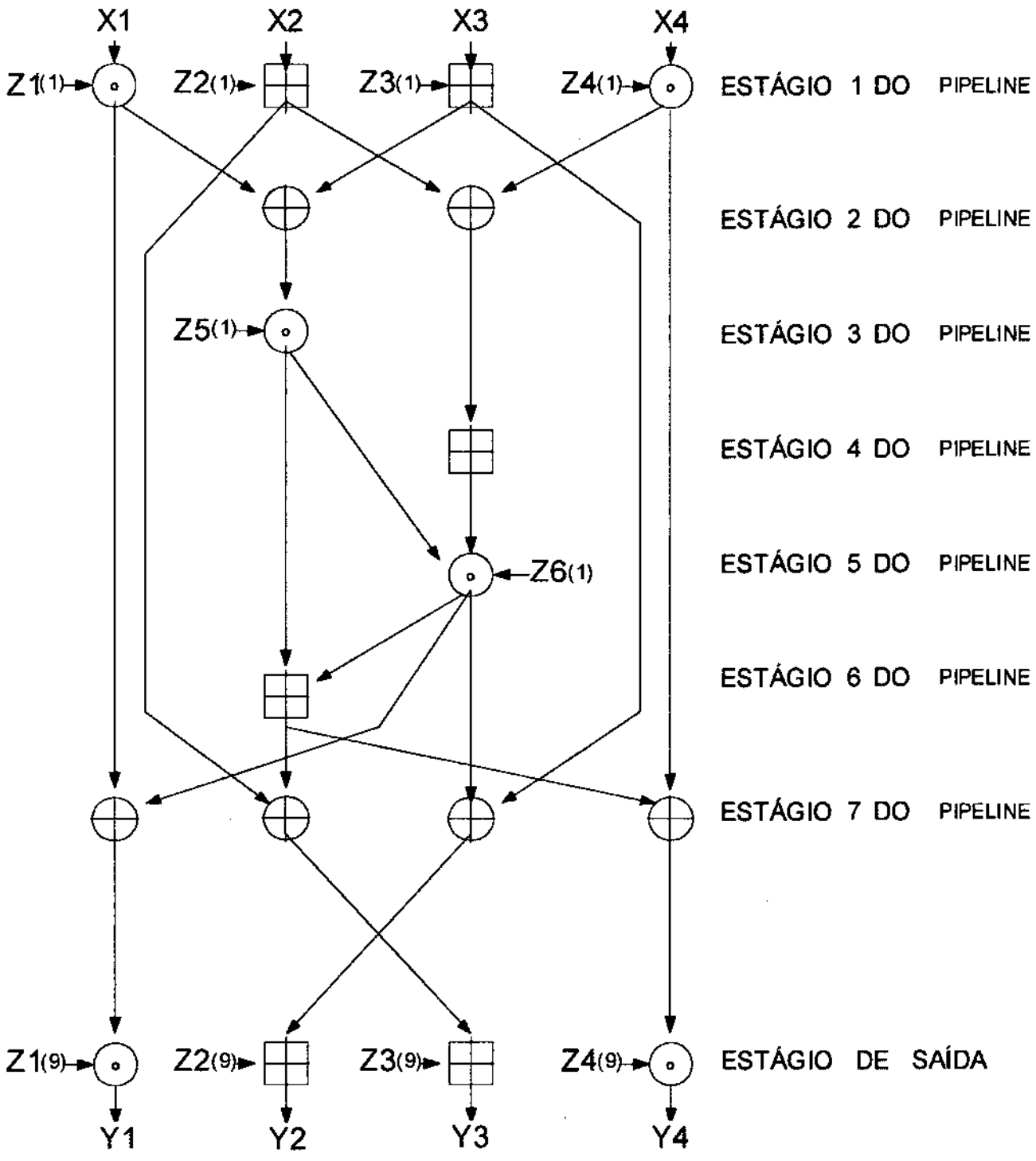


Figura 2

Arquitetura

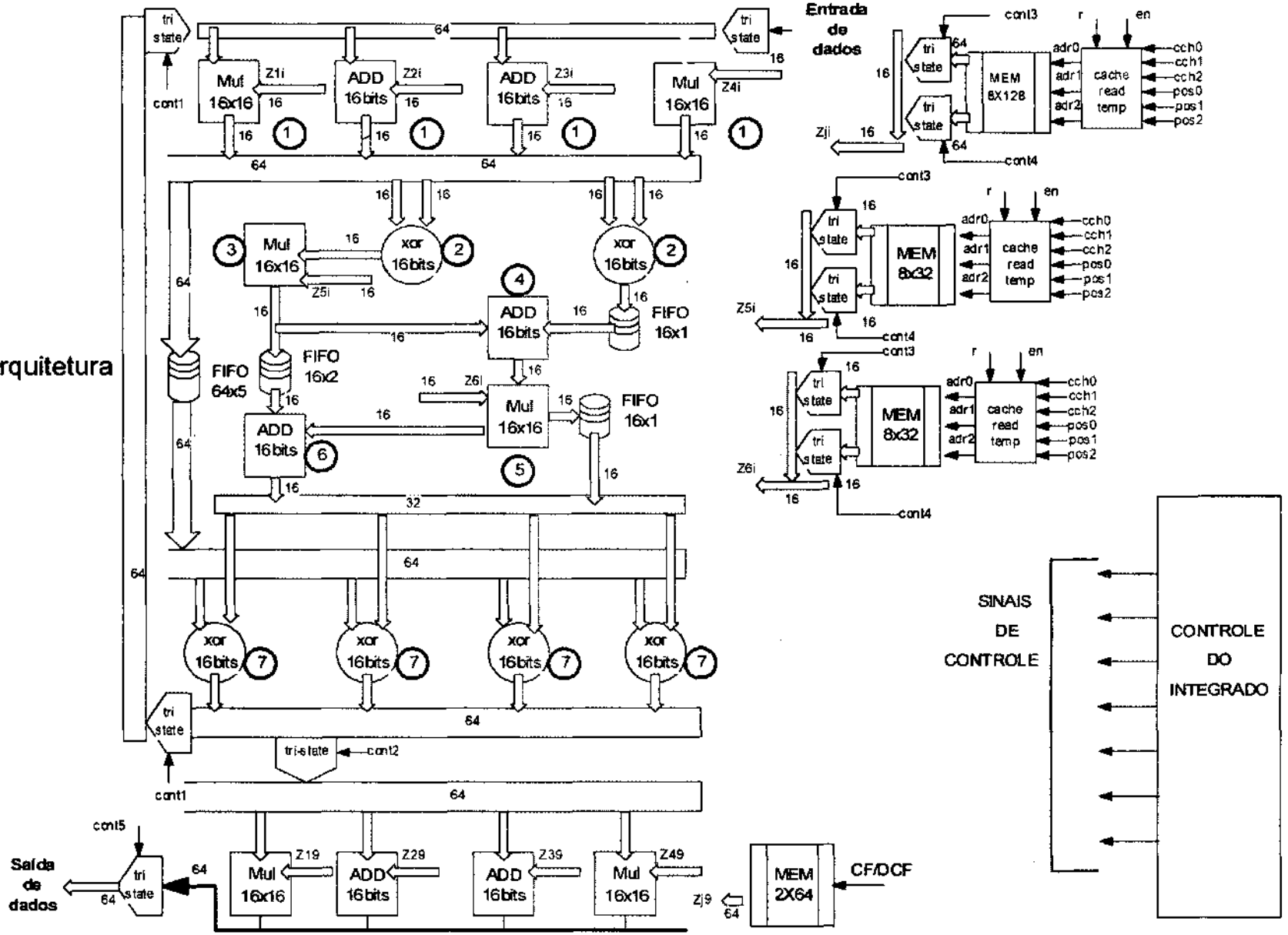


FIGURA 3

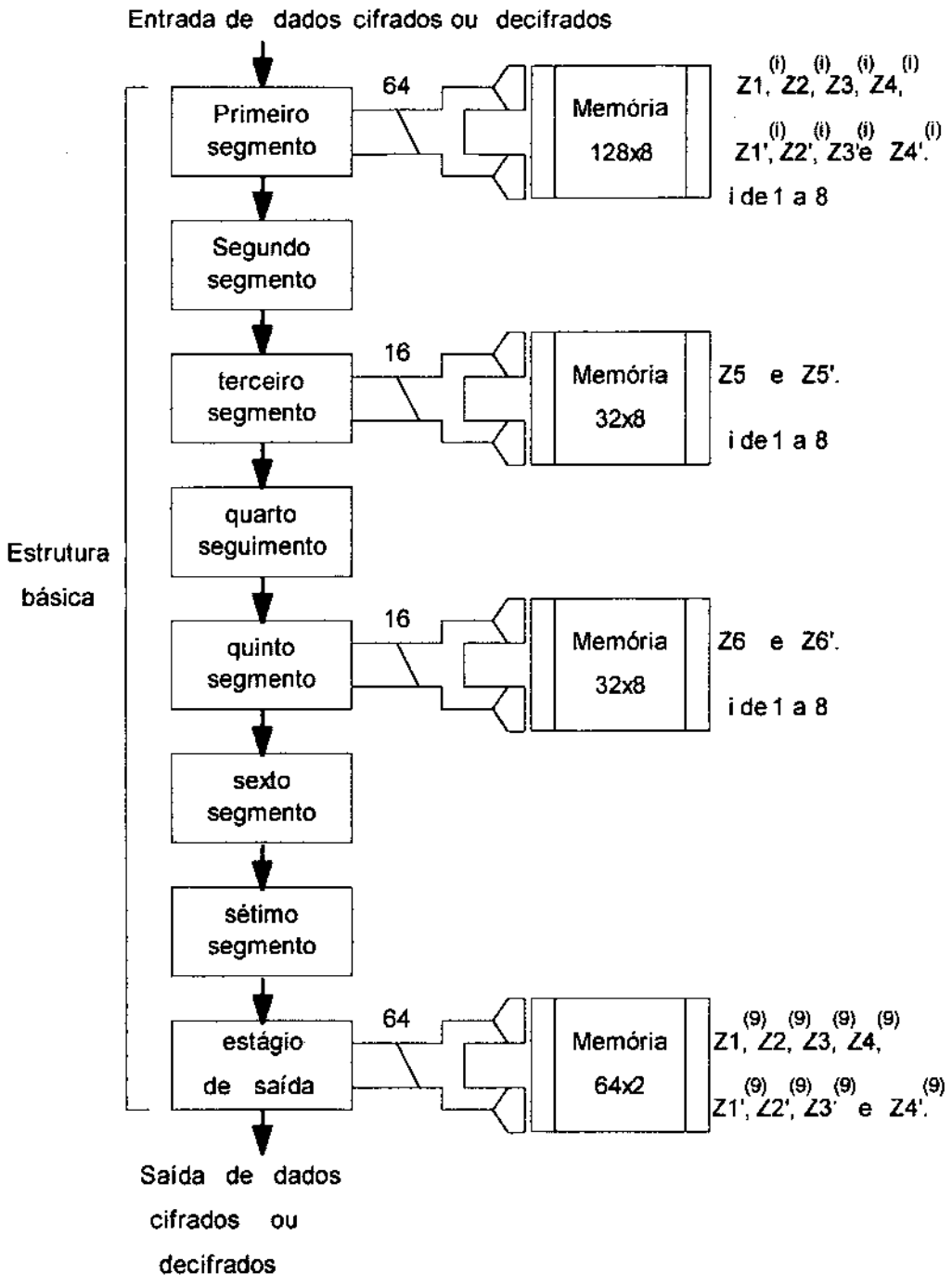


Figura 4

PI9903609

RESUMO

Patente de Invenção "PROCESSO DE IMPLEMENTAÇÃO EM HARDWARE DO ALGORÍTIMO CRIPTOGRÁFICO IDEA - HIPCRYPTO".

O HIPCrypto é a implementação em hardware do algoritmo de chave privada considerado mais seguro na atualidade, o algoritmo IDEA (International Data Encriyption Algorithm), através da exploração das técnicas de paralelismo espacial e temporal, de forma a atender as velocidades de processamento requeridas pelas redes do tipo ATM.